Deloitte.

Cloud Security

Ein umfassender Ansatz für den Schutz von Daten

13. Oktober 2023

MAKING AN IMPACT THAT MATTERS since 1845

Dipl.-Ing. Felix Lehner, BSc.

Allgemeines

- Felix Lehner ist **Senior Consultant** im **Infrastruktur & Cloud Security** Team von **Deloitte** Österreich
- Seit **2017** in der **Consulting** und **Auditing** Branche
- **Branchenfokus** liegt auf **Banken, Versicherungen und Chemie-Verarbeitungsunternehmen** in Europa

Professional Expertise & Achievements

- Durchführung **internationaler forensischen Untersuchungen**
- **Analyse- und Implementierungsprojekte** bei Unternehmen im Bereich **kritischer Infrastruktur** als Engagement Manager geleitet
- Unterstütze als **Solution Architect** bei der Sicherstellung der **GDPR** Compliance eines **SIEM / SOC**
- Überarbeitung des **Enterprise Security Management** eines **DAX-Konzerns**

Agenda

Deloitte Cyber at a Glance

Cloud

Deloitte Sovereign Cloud Architecture

Zahlen, Daten, Fakten | Weltweit führend im Bereich Cyber Risk Services

Die Cyber Risk Community von Deloitte unterstützt Unternehmen dabei, ihre strategischen Wachstums-, Innovations- und Performance-Ziele selbstbewusster zu verfolgen

 # 1 Weltweit führend im Bereich Security Consulting **zum 11. Mal in Folge**, nach Marktanteilen, im Jahr 2022

Quelle: Gartner, Market Share: Security Consulting Services, Worldwide, Elizabeth Kim, Shawn Eftink

12,500+

Cyber-Risiko Engagements im Jahr 2022 in allen wichtigen Branchen

Deloitte wird von Forrester zum 5. Mal in Folge als Leader im Bereich Information Security Consulting Services und in der Managed Security Services 2020 Vendor Assessment als Leader eingestuft

Quelle: The Forester Wave: Global Cybersecurity Consulting Providers, Q2 2019

Quelle: IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment by Martha Vazquez, September 2020.

1,400+

Certified Information Systems Security Specialists (CISSPs)

"Deloitte verfügt über umfassende Erfahrung, eine breite Palette von Managed Security Services und ein großes Ökosystem von Anbieterpartnerschaften."

Quelle: IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment by Martha Vazquez, September 2020.

Built by our people

21,000 (380 in AT & DE)
Risikomanagement- und Sicherheitsexperten durch das weltweite Deloitte Touche Tohmatsu Limited (DTTL) Netzwerk

30+
Cyber Intelligence Centers

150+
Zertifizierte Datenschutzexperten (CIPPs)

5+
Regional Delivery Centers

7,000+
Global Cyber Risk Experten
Untersützt von 10,000+
Experten mit Fokus in IT-Security in anderen Unternehmensbereichen

Zusammenarbeit mit führenden Regierungsbehörden und Branchenverbänden im Bezug auf Cyber Security Standards, fortschrittlicher Bedrohungsbekämpfung und Widerstandsfähigkeit

EMEA Cybersphere Center

1000+ Experten
28+ Nationalitäten

217+ managed security services engagements

26
Länder kollaborieren mit dem ECC im 2Q FY19
(70% Wachstumsrate)

SOC (Security Operation Center) mit hohen Qualitätsstandards:
FIRST® CERT®
ISO 22301®
ISO 27001®

Deloitte Cyber | Unsere Leistungen

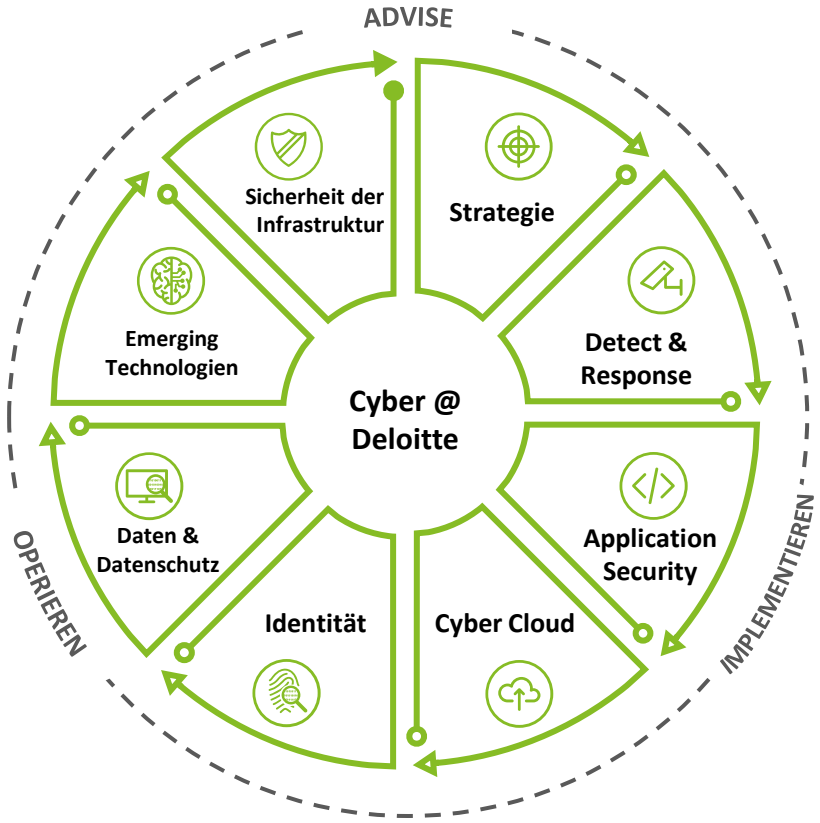
Wir betreuen unsere Kunden von der Strategieentwicklung und Kommunikation bis hin zu Ethical Hacking und Pen-Tests in allen Bereichen des Cyberspace

SICHERHEIT DER INFRASTRUKTUR: Wir sorgen für die Ausfallsicherheit der Kerntechnologie unserer Kunden wie Infrastruktur, Endgeräte und erweiterte Netzwerke.

NEUE TECHNOLOGIEN: Wir begleiten Unternehmen von der strategischen Ausrichtung bis hin zur Architekturentwicklung von neuen Technologien.

DATEN & DATENSCHUTZ : Mit unserer interdisziplinären Kompetenz bieten wir Sicherheit bei der Umsetzung von Datenschutzanforderungen.

IDENTITÄT: Wir unterstützen die Definition, Implementierung und den Betrieb einer IAM-Strategie, die auf die spezifischen Bedürfnisse unserer Kunden zugeschnitten ist.



STRATEGIE: Wir unterstützen Sie bei der Konzeption und Umsetzung ganzheitlicher strategischer Cyber-Transformationen im Einklang mit den Zielen unserer Kunden.

CYBER-ERKENNUNG & -REAKTION: Wir helfen Unternehmen dabei, ihre Widerstandsfähigkeit durch gezielte Maßnahmen angemessen zu verbessern.

ANWENDUNGSSICHERHEIT: Wir unterstützen unsere Kunden bei der Gewährleistung der Sicherheit ihrer Anwendungen, der Minimierung von Risiken und der Einhaltung von Vorschriften.

CYBER CLOUD: Wir ermöglichen es Unternehmen, Cloud-Lösungen in einem dynamischen Umfeld sicher zu nutzen und deren Potenziale voll auszuschöpfen.

Agenda

Deloitte Cyber at a Glance

Cloud

Deloitte Sovereign Cloud Architecture

Die Welt um uns herum verändert sich

Die zunehmende Geschwindigkeit der Digitalisierung verändert unsere Geschäftsmodelle, die Art und Weise, wie wir arbeiten, und führt zu immer mehr internen und externen Herausforderungen, denen wir uns stellen müssen

Digitale Transformation

Regulierung

Nachhaltigkeit

Mobile Arbeitskräfte

Globale Lieferketten

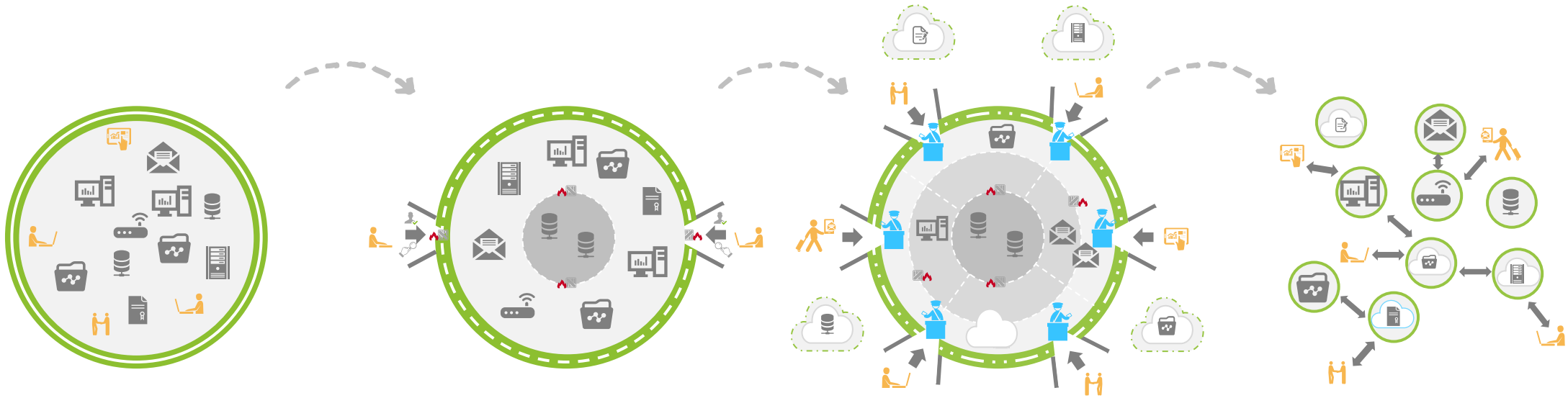
Ökosysteme

Die Entwicklung der Cyber Security

Geschäftsanforderungen und Trends haben die Cybersicherheitsstrategie, organisatorische und technologische Architektur sowie deren darunterliegenden Infrastruktur in den letzten Jahrzehnten stark verändert

1980 — *1990* — *Today* — *Tomorrow*

Perimeter Security » **Defense in Depth** » **Hybrid Cyber** » **Zero Trust Cyber Security**



Durch **Abgrenzung und physische Sicherheitskontrollen** geschützte Informationsbestände

Breakouts für Internetzugang und Kommunikation, Kontrolle durch mehrschichtige logische **Sicherheitskontrollen**. Mehr Sicherheitsbereiche - Nord/Süd-Schutz

Erhöhte Anzahl von Breakouts zur Unterstützung hybrider Umgebungen (z. B. Cloud/SaaS) und **erhöhte Abhängigkeit von der Überwachung**. Ost/West-Schutz

Die Grenzen des Netzes sind aufgehoben. **Trust** wird bei jeder Interaktion hergestellt und ständig neu bestätigt

Kritische Erfolgsfaktoren für die digitale Transformation

Die folgenden Bereiche müssen für eine erfolgreiche, sichere Anwendungsmigration oder -modernisierung berücksichtigt werden

Menschen

- Stakeholder Identifizierung
- Leadership Unterstützung
- Qualifiziertes Team
- Security Operating Modell

Prozesse

- Cloud Sicherheitskontrolle Definition & Instandhaltung
- Onboarding-Prozess der Applikation
- Kontinuierlicher Workflow zur Einhaltung von Kontrollen
- Prozess des Krisenmanagements

Technologie & Tools

- Security Architecture
- Rationalisierung der Cloud-Security Kapazitäten
- Datenschutz
- Identity und Access Management
- Zero Trust

Cloudsicherheit in Zahlen

Da Kunden ihre IT-Umgebungen modernisieren und zunehmend in die Cloud migrieren, müssen sie sich mit einer Vielzahl von Cyberrisiken auseinandersetzen

60 %

Die Kosten für Datenschutzverletzungen sind mit vollständig implementierter Sicherheitsautomatisierung um 60 % niedriger als ohne

49 %

Die öffentliche Cloud wird bis 2025 voraussichtlich 49 % der weltweit gespeicherten Daten ausmachen.

70 %

70 % der Unternehmen, die Daten/Workloads in der öffentlichen Cloud hosten, haben einen Sicherheitsvorfall erlebt.

47 %

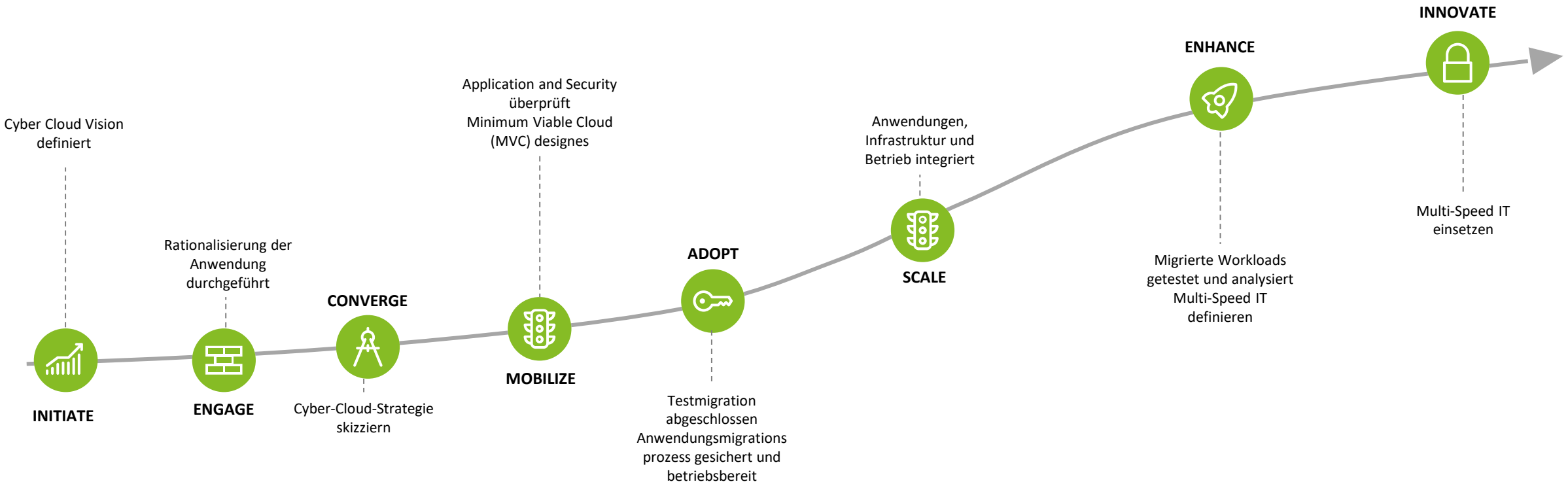
Schätzungsweise wissen 47 % der Führungskräfte nicht, welche Vorschriften und Standards für die Informationssicherheit und den Datenschutz gelten.

Herausforderungen der Cloudsicherheit

- **Compliance**
- **Datensicherheit**
- **Fehlende Cyber-Cloud Kompetenzen**
- **Geschwindigkeit & Sicherheit**
- **Dynamische Identität & Access Models**

Die Sicherheit muss in jeder Phase der Cloud-Reise eine Rolle spielen

Unternehmen müssen die Sicherheit in jeder Phase ihrer Cloud-Entwicklung miteinbeziehen, um den Cloud-Betrieb zu schützen und proaktiv gegen unerwünschte Cyber-Vorfälle zu verteidigen



Cloud Sicherheit & Sovereignty

Die wichtigsten Faktoren für eine Sichere und erfolgreiche Cloud Strategy

SOUVERÄN

- Sichere Ausführung von Anwendungen in isolierten Umgebungen (z.B. Enclaves)
- Mehrstufiges Sicherheitskonzept durch Kompartmentierung (ZeroTrust)
- Datenschutz auch außerhalb der nationalen Grenzen durch starke physische Absicherung & Verschlüsselung

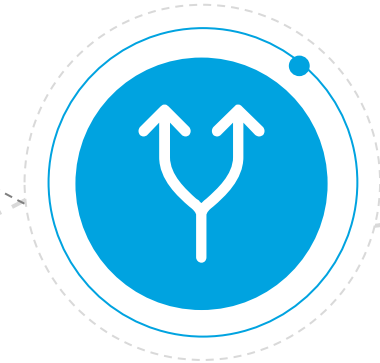
SICHER

- Verschlüsselte Daten & Kommunikation
- Hardware mit eingebauter Crypto-Technik
- BSI-zertifizierbare Lösungen
- Echtzeitsteuerung aller Komponenten

HYBRID

- Erweiterung der vorhandenen Private Cloud Angebote durch Public Cloud
- Integration vorhandener Lösungen einschließlich EDGE Komponenten

FLEXIBEL



- Nutzung von unterschiedlichen Cloud Lösungen je nach Sicherheitsanforderungen
- Geräte für den Einsatz zu Land/Wasser/Luft und extremen Bedingungen (Erdbeben, Flut)
- Lauffähig mit und ohne Cloud Connect

RESILIENZ

- Nutzung von vorhandenen Lösungen anderer Bündnispartner (EU, NATO etc.)
- Integration von Edge Komponenten für den Katastrophen- oder Militäreinsatz
- Umsetzung der NATO Vorgaben in einen sicheren „Building Block“

Cloud Sovereignty | Definition von Cloud Sovereignty

In Anbetracht unserer Forschung schlagen wir eine Definition der Cloud-Souveränität vor, die in Interviews mit KMUs vertieft werden sollte

UNSER DEFINITIONSVORSCHLAG

Refers to organizations' ability to **own, control and manage their data, computing resources and workloads in the cloud within a specific jurisdiction**, ensuring **regulatory compliance** and **without being dependent on service providers**. This concept involves issues of **data residency, access, privacy and security**, which are increasingly important as cloud adoption becomes more predominant across regions.

Key: Control and Choice | Jurisdiction/Geography | Data privacy & security | Technical applications | Regulatory compliance | Vendor independence

Agenda

Deloitte Cyber at a Glance

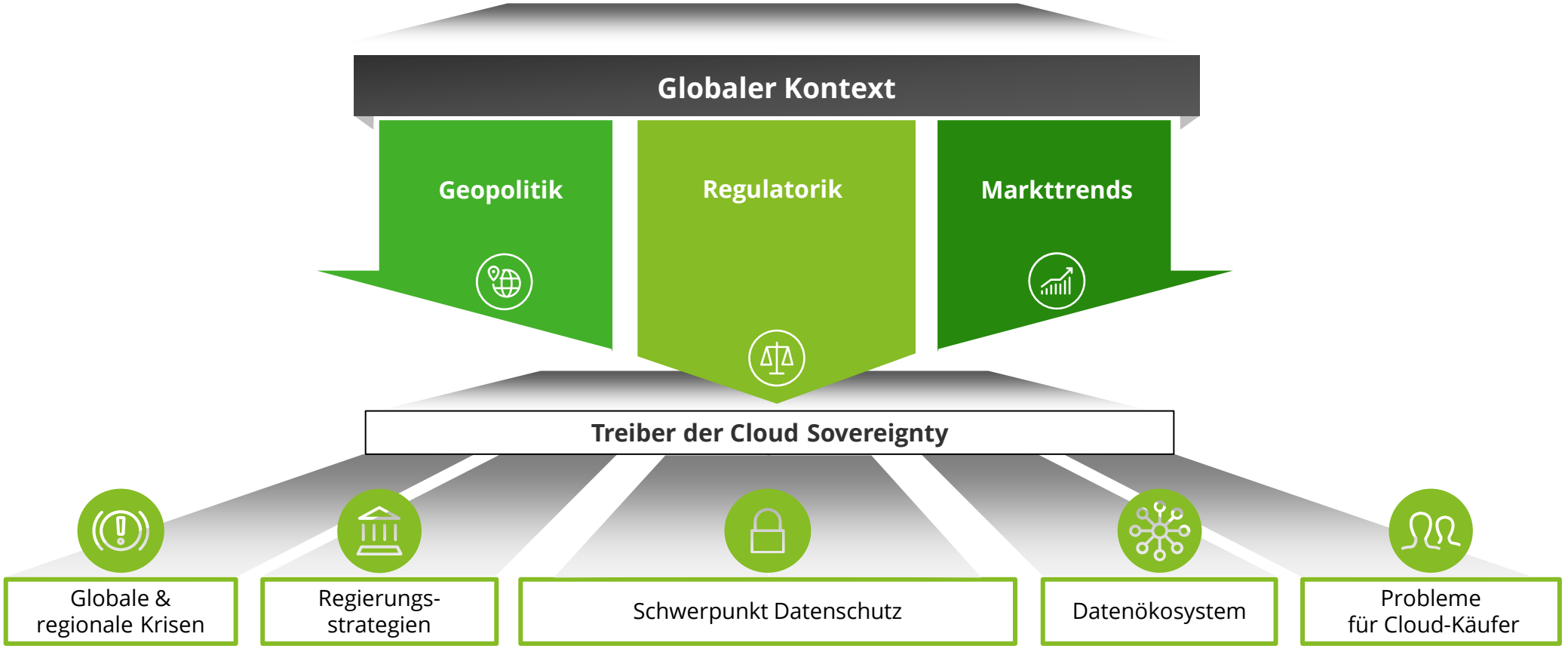
Cloud

Deloitte Sovereign Cloud Architecture

Deloitte Sovereign Cloud Architecture (SCA) | Einführung

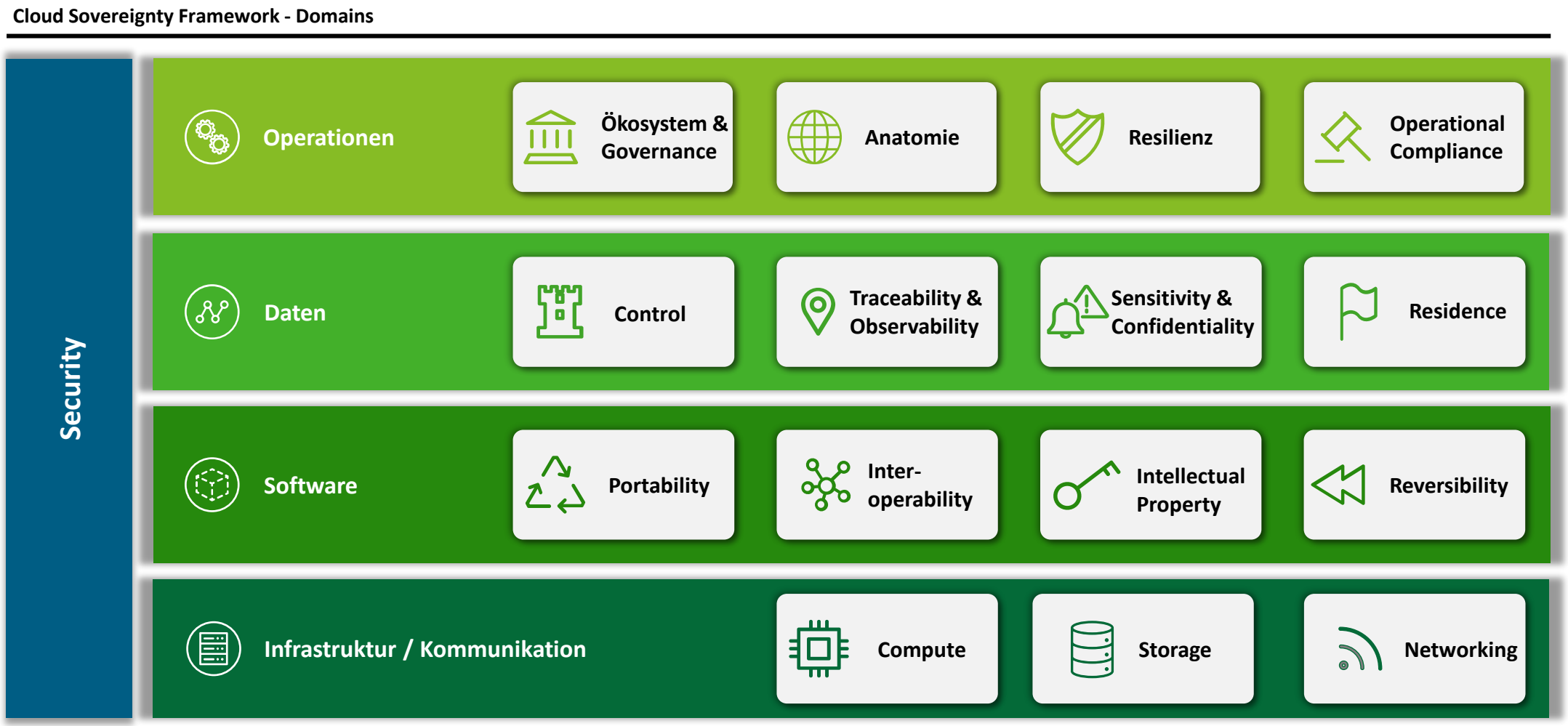
Relevante Aspekte von Cloud Sovereignty

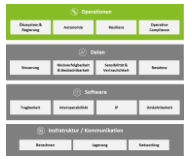
Cloud Sovereignty kann als die politischen, geschäftlichen und technologischen Dimensionen des Datenschutzes und der Datensicherheit beschrieben werden. Eine souveräne Cloud vereint Strategie, Governance und technische Kontrollen, um Widerstandsfähigkeit, Flexibilität, Autonomie und Einhaltung gesetzlicher Anforderungen sicherzustellen.



Cloud Sovereignty Framework - Überblick

Durch die Aufteilung von Domänen in bestimmte Bereiche können Unternehmen die Herausforderungen bei der Einführung von Souveränität in der Cloud besser verstehen.





Cloud Sovereignty Framework - Operations

Die operative Souveränität dreht sich um die notwendigen Fähigkeiten von Operations, um die Souveränität durch die Implementierung souveräner Richtlinien im Ökosystem der Cloud-Anbieter aufrechtzuerhalten.

Was ist operative Souveränität?

Dieser Bereich konzentriert sich darauf, **Transparenz und Kontrolle** über ihre **Provider-Aktivitäten** zu geben. Dies trägt dazu bei, unbefugten Zugriff auf ihre Daten zu verhindern, indem IT-Services sowie die zugrunde liegenden Konfigurationselemente überwacht und gesteuert werden, die für die sichere und effektive Bereitstellung und den Betrieb von Cloud-Services im Einklang mit den Souveränitätsrichtlinien erforderlich sind.

Insights

Unter den **Top 5** der **Entscheidungskriterien für IT-Investitionen** in Bezug auf digitale Souveränität *

- **"Präferenzen für die Zusammenarbeit mit lokalen/nationalen Anbietern/Dienstleistern"**
- **"Vorschriften für Geschäftskontinuität und Disaster Recovery"**

Operations subdomains

Ökosystem & Governance

Souveränitäts-Governance im Ökosystem der Cloud-Anbieter ist der Schlüssel zur Gewährleistung der föderierten Souveränität und der betrieblichen Nachhaltigkeit.

Anatomie

Fördern Sie interne Kapazitäten, um Lösungen effektiv und unabhängig von Cloud-Modell und -Anbieter auszuführen, und ermöglichen Sie gleichzeitig hybride Szenarien, um Innovationen und Funktionen aus der Public Cloud zu nutzen.

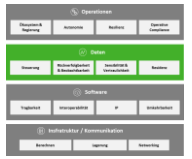
Resilienz

Fähigkeit, Risiken zu identifizieren, die sich auf die Servicekontinuität auswirken, sich von unerwünschten Ereignissen zu erholen und Cloud-Services weiterzuentwickeln, um zukünftige Unterbrechungen zu verhindern.

Operational Compliance

Operative Überwachung von regulatorischen Pflichten und Anbieterverträgen zur Einhaltung staatlicher Richtlinien und SLOs von Cloud-Anbietern.

Quelle: IDC's Future Enterprise Resiliency & Spending Survey – Wave 4, Mai 2022



Cloud Sovereignty Framework - Daten

Die Datenhoheit gewährleistet die Sicherheit und Integrität der Unternehmensdaten und stellt die wichtigste Ebene dar, um die Einhaltung der Vorschriften durch die Aufsichtsbehörden zu gewährleisten.

Was ist Datensouveränität?

Datensouveränität ist die Fähigkeit eines Unternehmens, die **Kontrolle über seine Daten zu behalten**, einschließlich des Ortes und der Art und Weise, wie sie gespeichert werden, wie sie geschützt und verarbeitet werden und wer Zugriff darauf hat. Unternehmen können nur dann die volle Datenhoheit erreichen, wenn sie der Dateneigentümer sind. Andernfalls sind sie auf Vereinbarungen und Verträge mit Dritten angewiesen, was den **Grad der Souveränität** einschränkt.

Insights

N°1

Einfluss auf die Technologieinvestitionen von Unternehmen im Zusammenhang mit **digitaler Souveränität.***

“Kontrolle über den Zugriff auf Daten durch die Administratoren von Cloud-Dienstanbietern”

Daten Sovereignty Subdomains

Control

Unternehmen müssen die Kontrolle darüber haben, wie ihre Daten verwendet, gespeichert und gesichert werden, um die Datenhoheit zu gewährleisten.

Traceability & Observability

Rückverfolgbarkeit ermöglicht es Unternehmen, Daten innerhalb ihrer IT-Landschaft zu verfolgen und zu bestimmen, wo sie gespeichert sind, die Beobachtbarkeit von Daten hilft zu verstehen, wie sie verwendet werden und wer darauf zugreift.

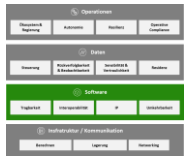
Sensitivity & Confidentiality

Die Klassifizierung von Daten auf ihrer Sensibilität und Vertraulichkeit trägt dazu bei, die Datensouveränität zu gewährleisten, da verschiedene Arten von Daten einem unterschiedlichen Sicherheitsniveau entsprechen.

Residence

Residenz ist die Fähigkeit, Daten sicher und datenschutzkonform zu speichern.

Quelle: IDC's Future Enterprise Resiliency & Spending Survey – Wave 4, Mai 2022



Cloud Sovereignty Framework - Software

Software-Souveränität ermöglicht es einem Unternehmen, seine Anwendungen auf verschiedene Software-Stacks zu migrieren, wenn sich der geschäftliche oder rechtliche Kontext ändert.

Was ist Software-Souveränität?

Software-Souveränität bezieht sich auf die Fähigkeit eines Unternehmens, Software oder Lösungen **unabhängig** von der **Produkt-Roadmap eines Herstellers** zu betreiben und zu orchestrieren. Dazu gehört die Kontrolle über den Quellcode, die Entwicklungsprozesse und Software-Updates sowie die Möglichkeit, zwischen den Plattformanbietern zu wechseln. Solche **Open-Source-Lösungen** bieten auch die Möglichkeit, auf vielen **verschiedenen Plattformen** ausgeführt zu werden.

Insights

N°1

Priorisierte Maßnahmen aufgrund zunehmender Bedenken hinsichtlich der **digitalen Souveränität durch Geschäfts- und IT-Führungskräfte.***

“Verbesserung der Datenschutzmaßnahmen und -umsetzung”

Software subdomains

Portability

Die Fähigkeit, Software auf verschiedenen (Cloud-)Plattformen auszuführen. Die Möglichkeit, Software neu zu verpacken und die Anbieterbindung für On-Premise, Hosting und IaaS/PaaS zu beseitigen.

Interoperability

Die Fähigkeit, verschlüsselte und geschützte Daten zwischen verschiedenen Systemen über mehrere Plattformen hinweg zuverlässig auszutauschen.

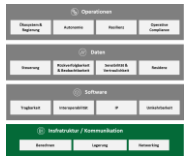
Intellectual Property

Die Fähigkeit, sich unter Berücksichtigung der rechtlichen Rahmenbedingungen nicht auf geistiges Eigentum zu verlassen, das von großen Softwareanbietern beeinflusst wird, und die Fähigkeit, an marktgetriebenen Innovationen teilzunehmen.

Reversibility

Die Möglichkeit, die Software zurück in eine On-Premise-Umgebung zu verlagern, wenn das Geschäfts- oder Risikomanagement dies erfordert.

Quelle: IDC's Future Enterprise Resiliency & Spending Survey – Wave 4, Mai 2022



Cloud Sovereignty Framework - Infrastruktur & Kommunikation

Infrastruktur- und Kommunikationsfunktionen sind der Schlüssel zum Aufbau sicherer, zuverlässiger und skalierbarer Cloud-Architekturen zur Unterstützung von Anwendungsfällen der Souveränität.

Was ist Infrastruktur- und Kommunikationssouveränität?

Infrastruktur und Kommunikation sind die **souveränen technischen Grundlagen** für die Betriebs-, Daten- und Softwareschichten als Wegbereiter, um die volle Kontrolle über sie zu haben.
Die Verwendung **offener Standards** für Infrastruktur und Kommunikation maximiert die **Anpassungsfähigkeit und Widerstandsfähigkeit** gegenüber dem Wechsel zwischen Souveränitätsszenarien.

Insights

Ganz oben bei den **Entscheidungskriterien für IT-Investitionen** in Bezug auf **digitale Souveränität.***

“Eigentum an der Cloud-Infrastruktur durch Anbieter in ausländischem Besitz”

Infrastruktur & Kommunikation Subdomains

Compute

Die offenen Standards, die in Compute-Instanzen verwendet werden, um verschiedene Systeme miteinander zu verbinden.

Storage

Die Möglichkeit, den Compute-Anbieter auszuwählen oder die Rechenleistung selbst bereitzustellen.

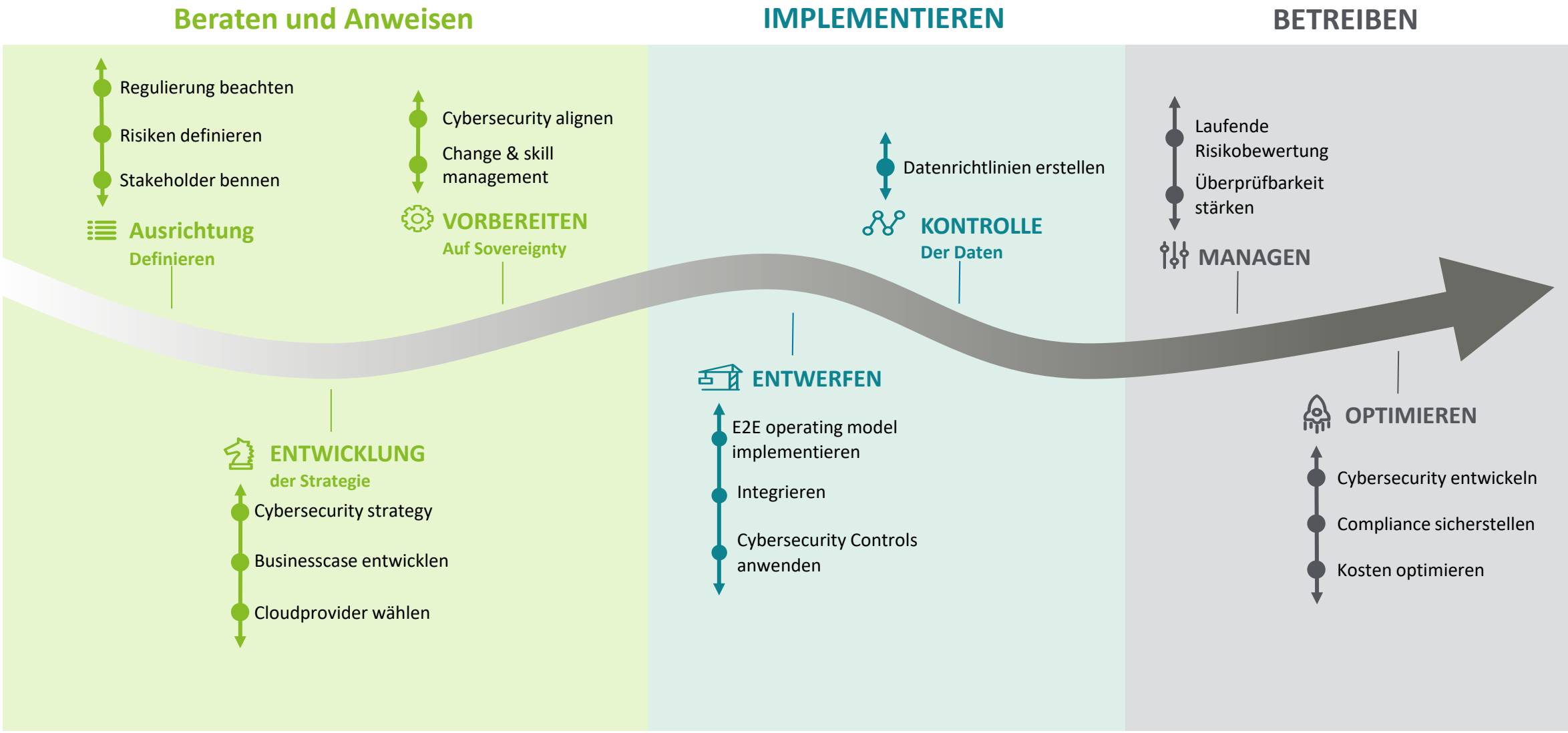
Networking

Die Fähigkeit, Daten zwischen Repositories (On-Premise, Cloud, Edge) zu verbinden und zu übertragen.

Quelle: IDC's Future Enterprise Resiliency & Spending Survey – Wave 4, Mai 2022

Der Weg zu Cloud Sovereignty

Wie eine klassische Cloud Sovereignty Roadmap aussehen kann



Deloitte.